Fact Sheet on Department of Justice Cyber-Digital Task Force Report

The Attorney General established the Department of Justice's Cyber-Digital Task Force in February 2018 and directed the Task Force to answer two questions: (1) how the Department is currently combating the global cyber threat, and (2) how federal law enforcement can more effectively accomplish its mission in this vital and evolving area. On July 19, 2018, the Cyber-Digital Task Force is making public its initial report, which describes how the Department responds to current cyber threats.

The Global Cyber Threat

Cyber-enabled attacks are exacting an enormous toll on American businesses, government agencies, and families. These attacks have resulted in billions of dollars in losses and have fostered efforts by hostile foreign governments to undermine American institutions and democracy. The Cyber-Digital Task Force Report details how the Department of Justice is combating these malicious, cyber-enabled threats.

Countering Malign Foreign Influence Operations

The Report begins in Chapter 1 by focusing on one of the most pressing cyber-enabled threats confronting our Nation: the threat posed by malign foreign influence operations. Malign foreign influence operations include covert actions by foreign governments intended to sow division in our society, undermine confidence in our democratic institutions, and otherwise affect political sentiment and public discourse to achieve strategic geopolitical objectives.

Chapter 1 categorizes malign foreign influence operations and explains how these operations can target our Nation's democratic institutions, including our elections. It ends by describing the Department's efforts to protect the 2018 midterm elections and other future elections.

The five types of malign foreign influence operations the Report identifies include:

- Cyber operations targeting election infrastructure, such as voter registration databases, voting machines, or other critical infrastructure;
- Cyber operations targeting political organizations, campaigns, and public officials, such as those carried out by Russian intelligence officers, as alleged in a July 2018 indictment;
- Covert influence operations to assist or harm political organizations, campaigns, and public officials, such as those detailed in a February 2018 indictment of 13 Russian nationals alleging covert activities and financial support to unwitting U.S. persons;
- Covert influence operations, including disinformation operations, to influence public opinion and sow division, such as the operation of social media pages and other forums that spread disinformation and divisive messaging to U.S. audiences; and
- Overt influence efforts, such as the use of lobbyists, foreign media outlets, and other organizations to influence policymakers and the public.

The Report marks the first time the Department has publicly articulated the types of threats posed by malign foreign influence operations and formally described how, in coordination with other federal departments and agencies, it is responding to these operations.

The response is five-fold:

- Aggressively investigating and prosecuting criminal activity where appropriate, and promoting compliance with, and punishing violations of, the Foreign Agents Registration Act (FARA).
- Working collaboratively with other executive departments, including the Department of Homeland Security (DHS), to share information about threats and vulnerabilities with State and local election officials, political organizations, and other potential victims, so they can detect and prevent operations that target them.
- Supporting other executive departments' actions, such as financial sanctions or diplomatic and intelligence efforts.
- Forming and maintaining strategic relationships with social media providers to assist those companies in their voluntary efforts to identify malign foreign influence activity and to enforce terms of service that prohibit the use of their platforms for such activity.
- Using information developed in our investigations to protect the public by, where appropriate, exposing the nature of the foreign influence threat. The Report announces a new Department policy governing the disclosure of foreign influence operations (pages 16-17).
    - This policy provides guideposts for Department action to expose and thereby counter foreign influence threats, consistent with the fundamental principle that the Department always must seek to act in ways that are politically neutral, compliant with the First Amendment, and designed to maintain the public trust.

The Report also outlines the Department's framework to counter malign foreign influence operations ahead of the 2018 midterm elections, and describes the work of the FBI's Foreign Influence Task Force, which integrates the FBI's cyber, counterintelligence, counterterrorism, and criminal law enforcement resources towards a better understanding of the threats posed by malign foreign influence operations. The FBI coordinates with other national security agencies and develops strategic relationships with State and local authorities, international partners, and the private sector, in a comprehensive approach to combating the foreign influence problem.

As the Report observes, the Department of Justice plays an important role in combating foreign efforts to interfere in our elections, but it cannot alone solve the problem. There are limits to the Department's role—and the role of the U.S. government—in addressing foreign influence operations aimed at sowing discord and undermining our Nation's institutions. Combating foreign influence operations requires a whole-of-society approach that relies on coordinated actions by federal, State, and local government agencies; support from potential victims and the private sector; and the active engagement of an informed public.

Other Significant Cyber Threats

In Chapters 2 and 3, the Report discusses other significant cyber-enabled threats confronting our Nation, including attacks intended to damage computer systems; data theft; fraud schemes; crimes threatening personal privacy, such as sextortion and other forms of blackmail and harassment; and attacks on critical infrastructure. Each of these threats is serious, and the Report

details the important work that the Department of Justice is doing to keep America safe in the face of these complex and evolving threats.

Chapter 4 of the Report details how the Federal Bureau of Investigation responds to cyber incidents, while Chapter 5 focuses on how the Department manages and trains its workforce on cyber matters. Finally, the Report concludes in Chapter 6 with observations about certain priority policy matters, and identifies eight non-exclusive areas for deeper evaluation (pp. 125-26), charting a path for the Cyber-Digital Task Force's future work.